IN THE DRAWINGS

A full set of drawings including corrections and the required additions are included herewith.

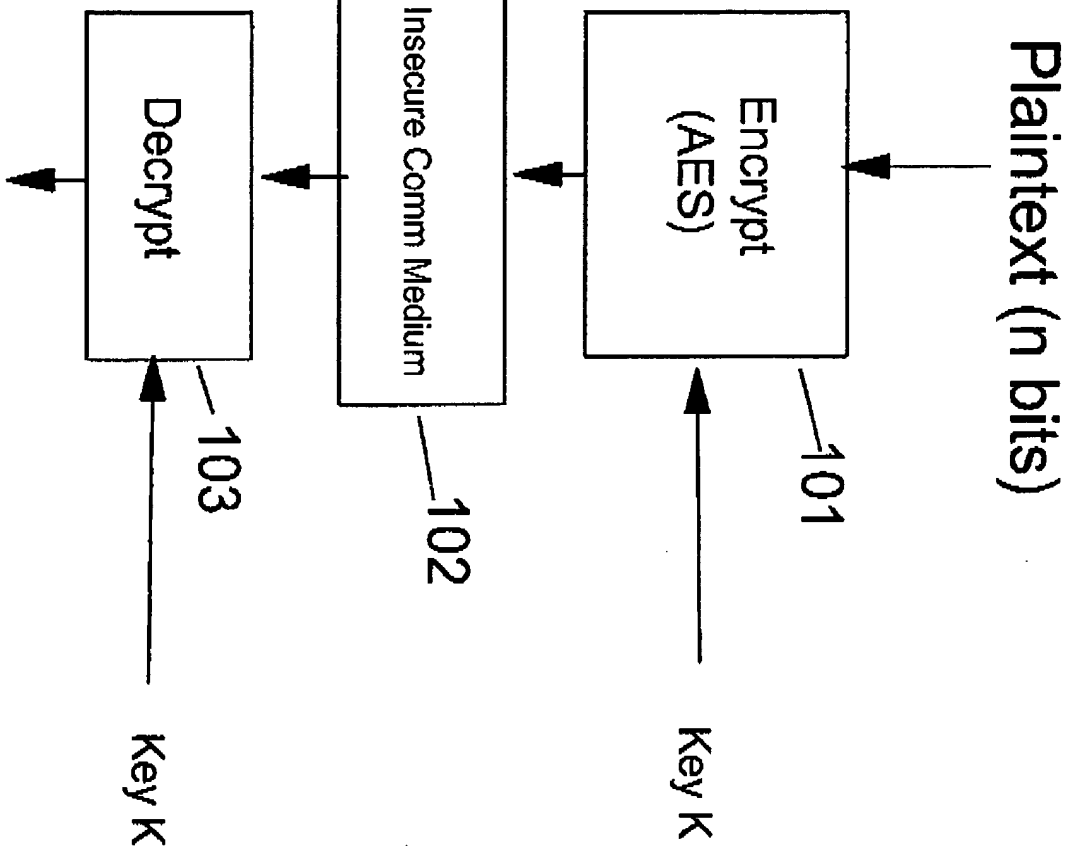


Fig. 1 (Prior Art)

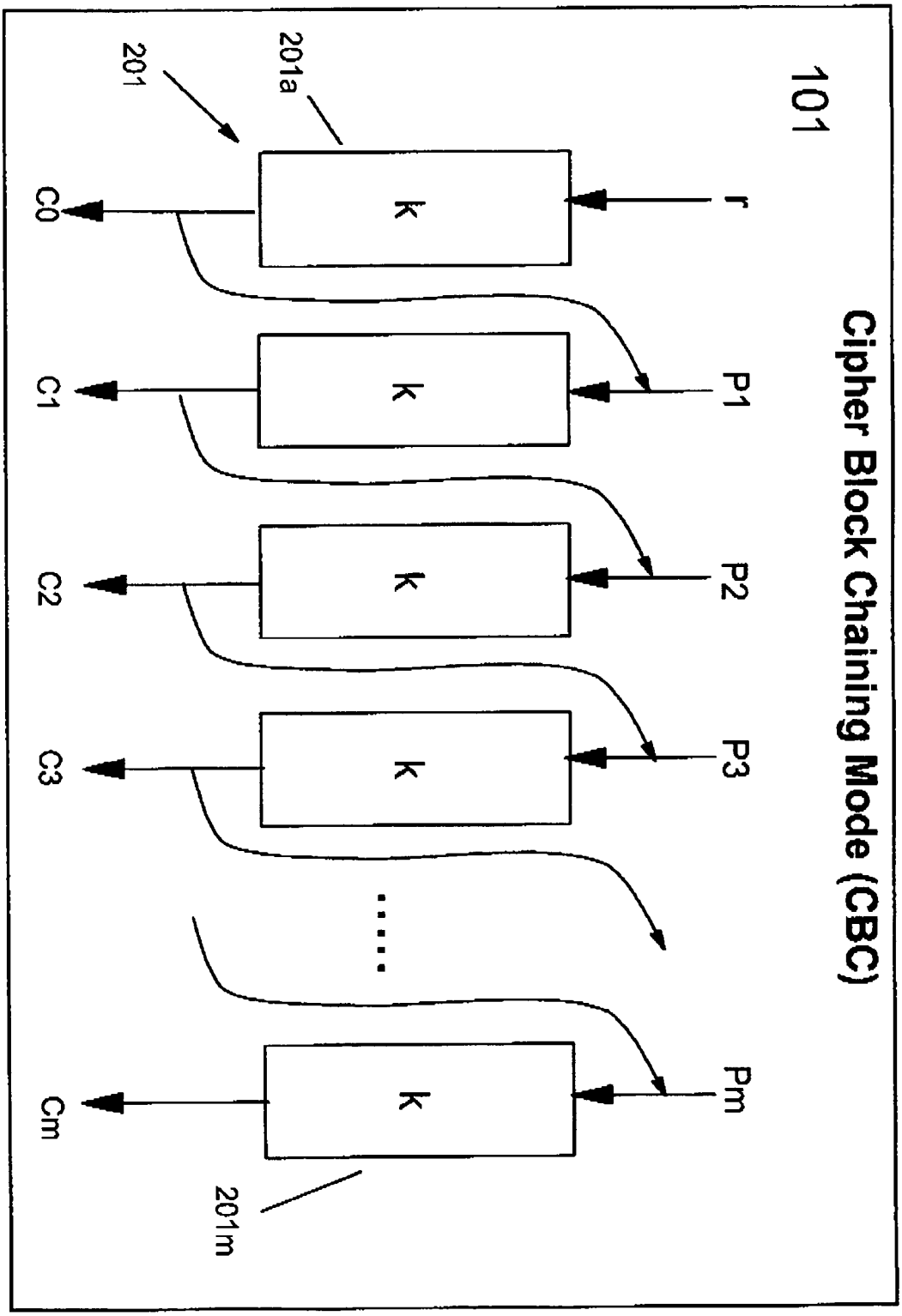


Fig. 2 (Prior Art)

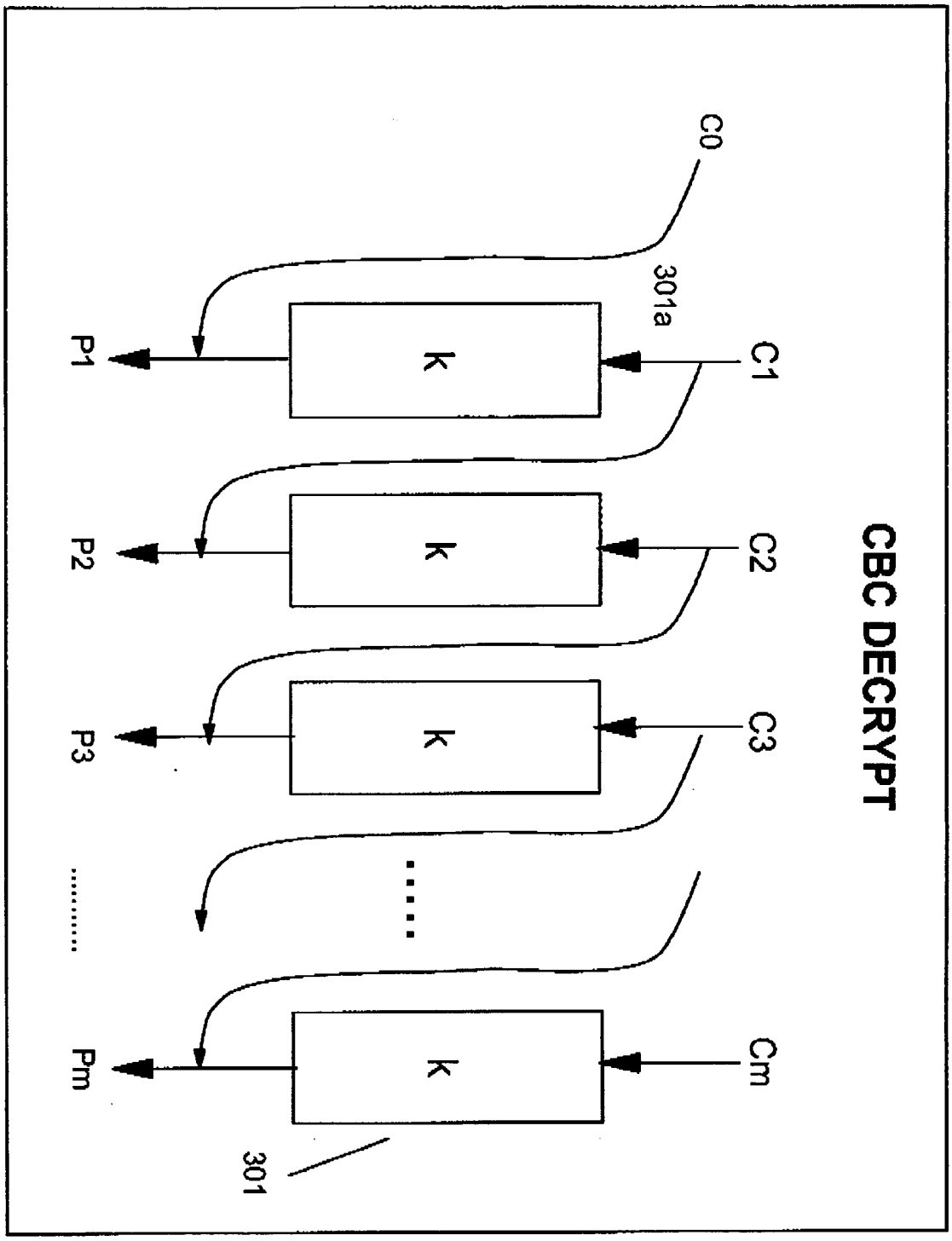


Fig. 3 (Prior Art)

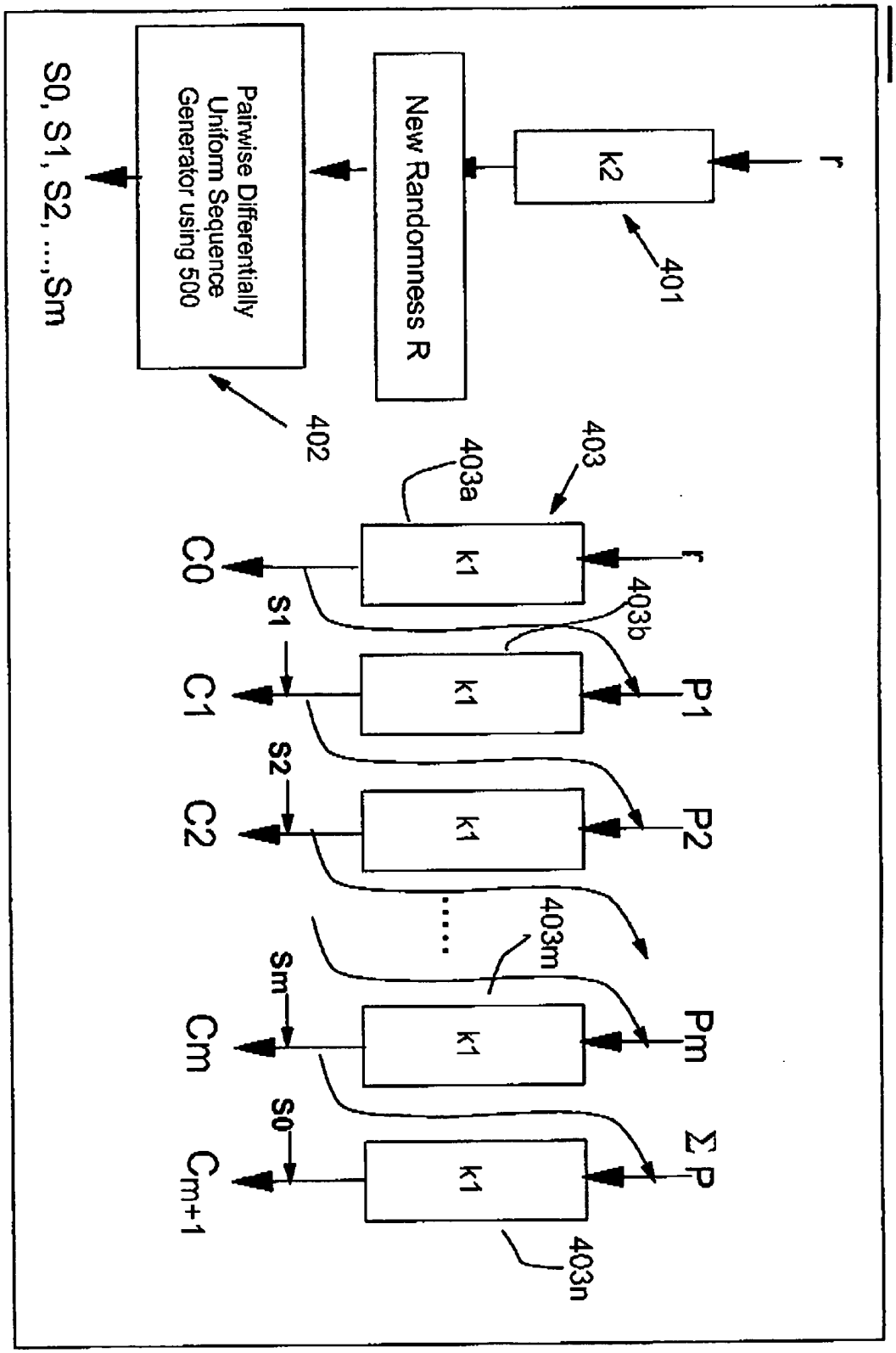
400
r
k2
401
New Randomness R
Pairwise Differentially Uniform Sequence Generator using 500
S0, S1, S2, ...,Sm
402
403
403a
403b
403m
403n
k1
C0
C1
C2
Cm
Cm+1
S0
S1
S2
Sm
P1
P2
Pm
ΣP
.....

Fig. 4

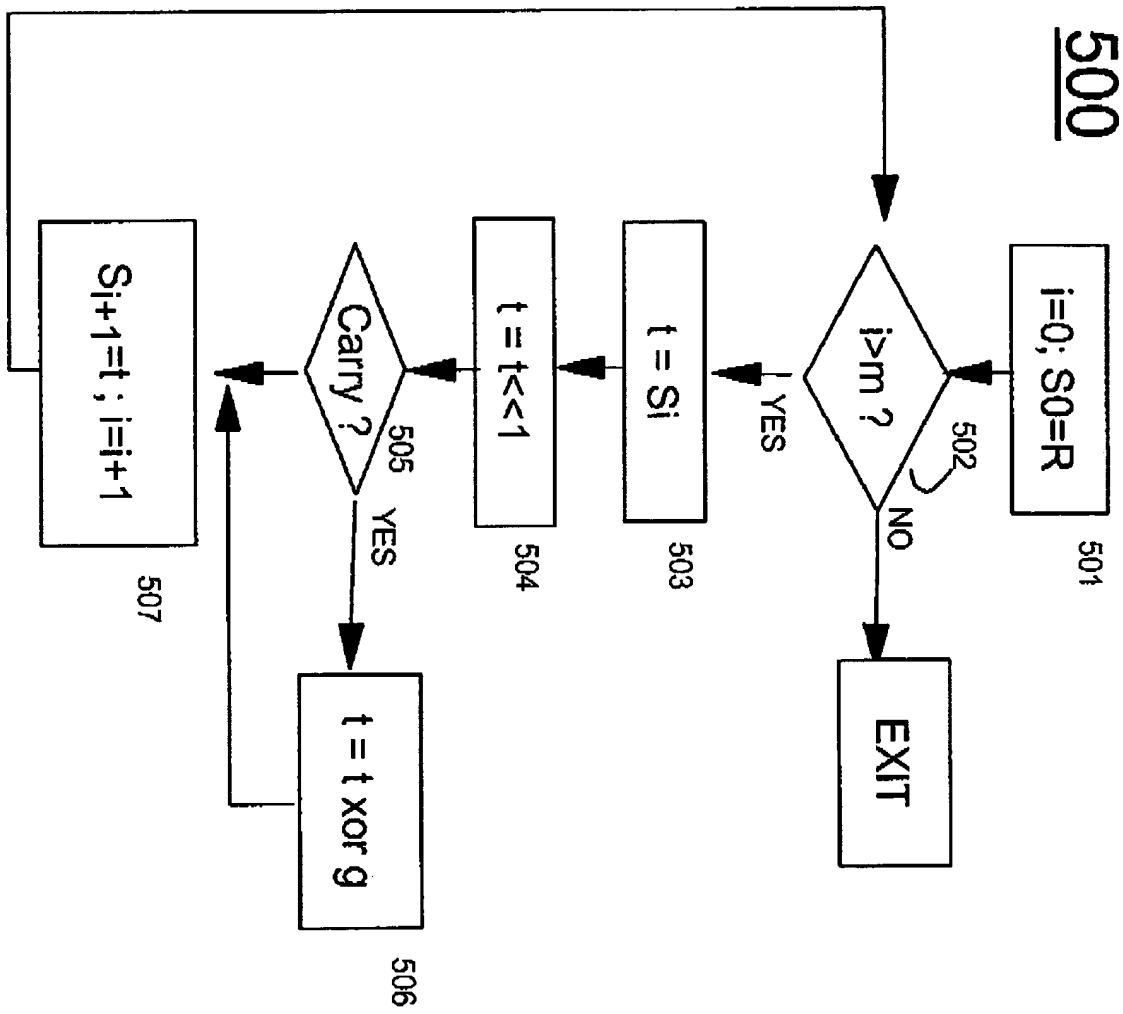
500
i=0; S0=R
501
i>m ?
502
NO
YES
EXIT
t = Si
503
t = t<<1
504
Carry ?
505
YES
t = t xor g
506
Si+1=t ; i=i+1
507

Fig. 5

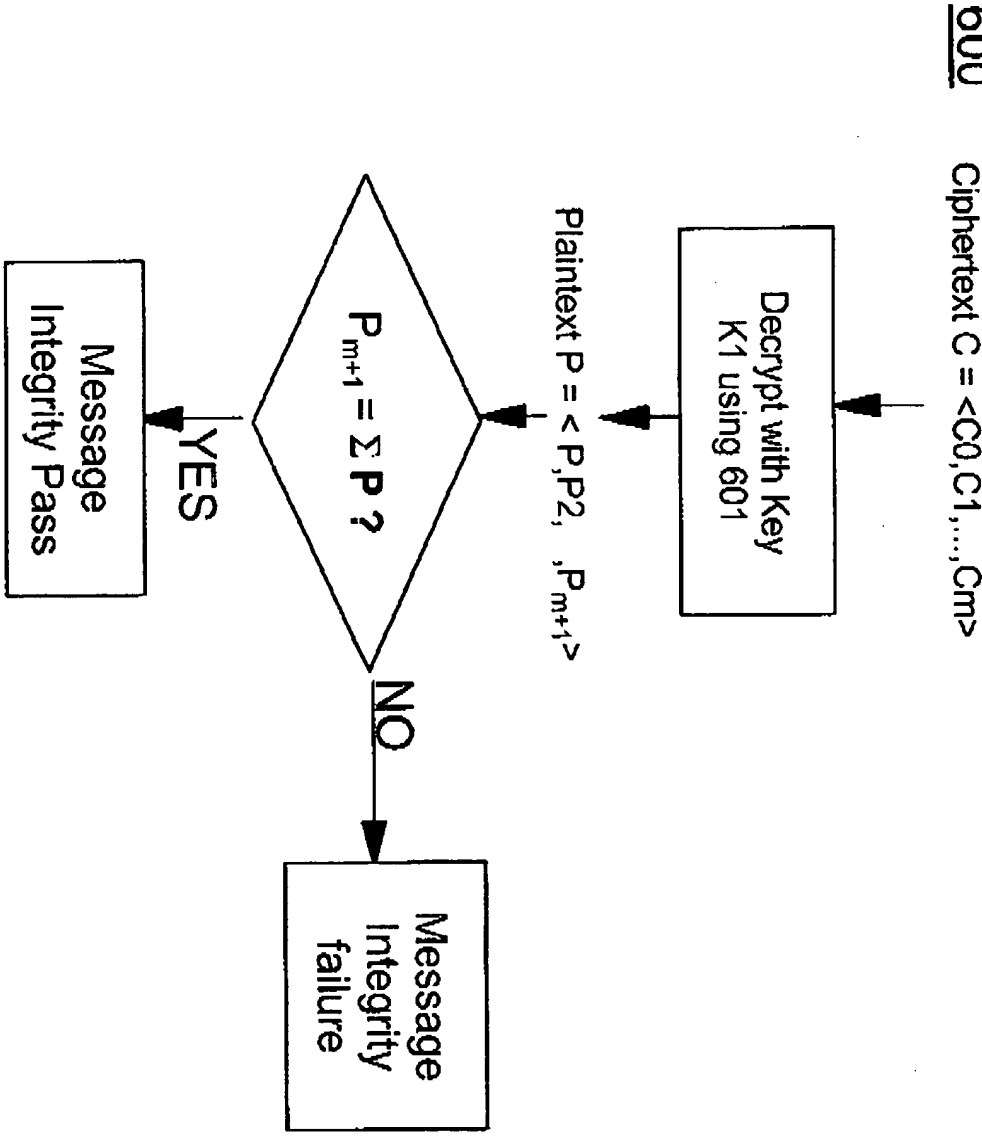
600
Ciphertext C = <C0,C1,...,Cm>
Decrypt with Key K1 using 601
Plaintext P = < P,P2, ,Pm+1>
Pm+1 = Σ P ?
YES
Message Integrity Pass
NO
Message Integrity failure

Fig. 6

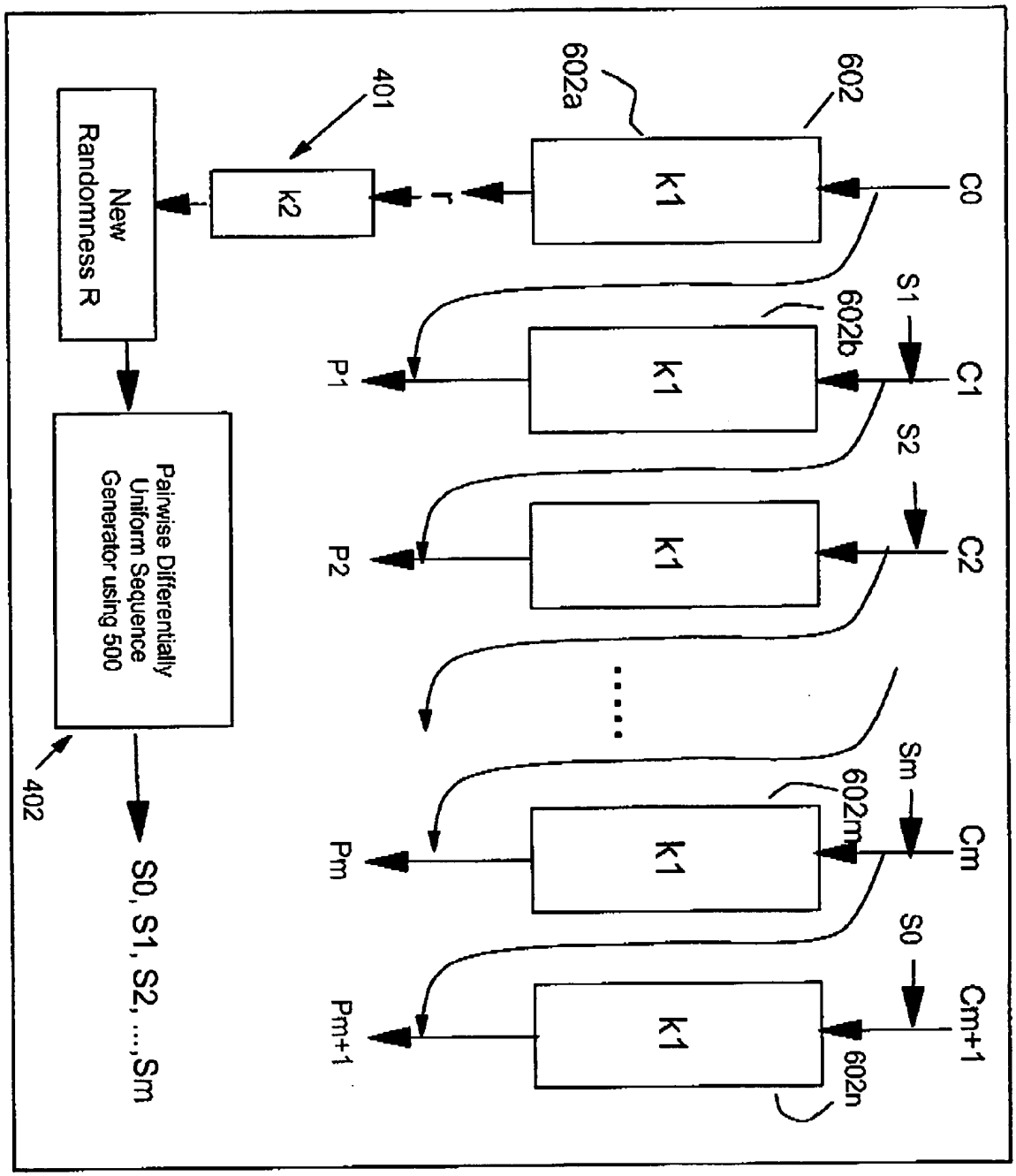
601
602
602a
401
k1
k2
r
C0
New Randomness R
S1
602b
P1
C1
S2
P2
C2
Pairwise Differentially Uniform Sequence Generator using 500
Sm
602m
Pm
Cm
S0
Pm+1
Cm+1
602n
402
S0, S1, S2, ...,Sm

FIG. 7

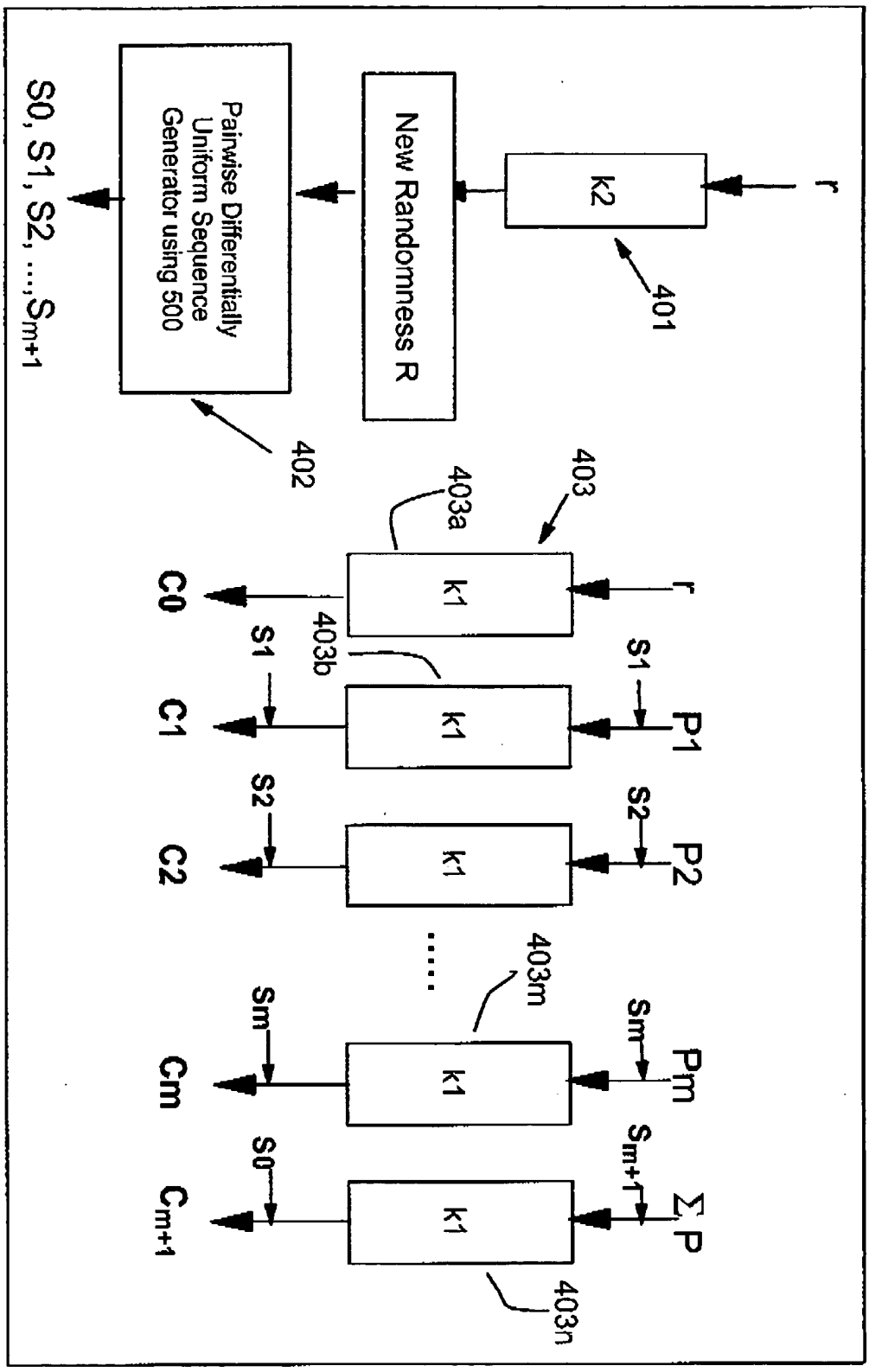
800
r
k2
401
New Randomness R
Pairwise Differentially Uniform Sequence Generator using 500
S0, S1, S2, ...,Sm+1
402
403
403a
403b
403m
403n
k1
C0
C1
C2
Cm
Cm+1
S1
S2
Sm
S0
P1
P2
Pm
ΣP
Sm+1

Fig. 8

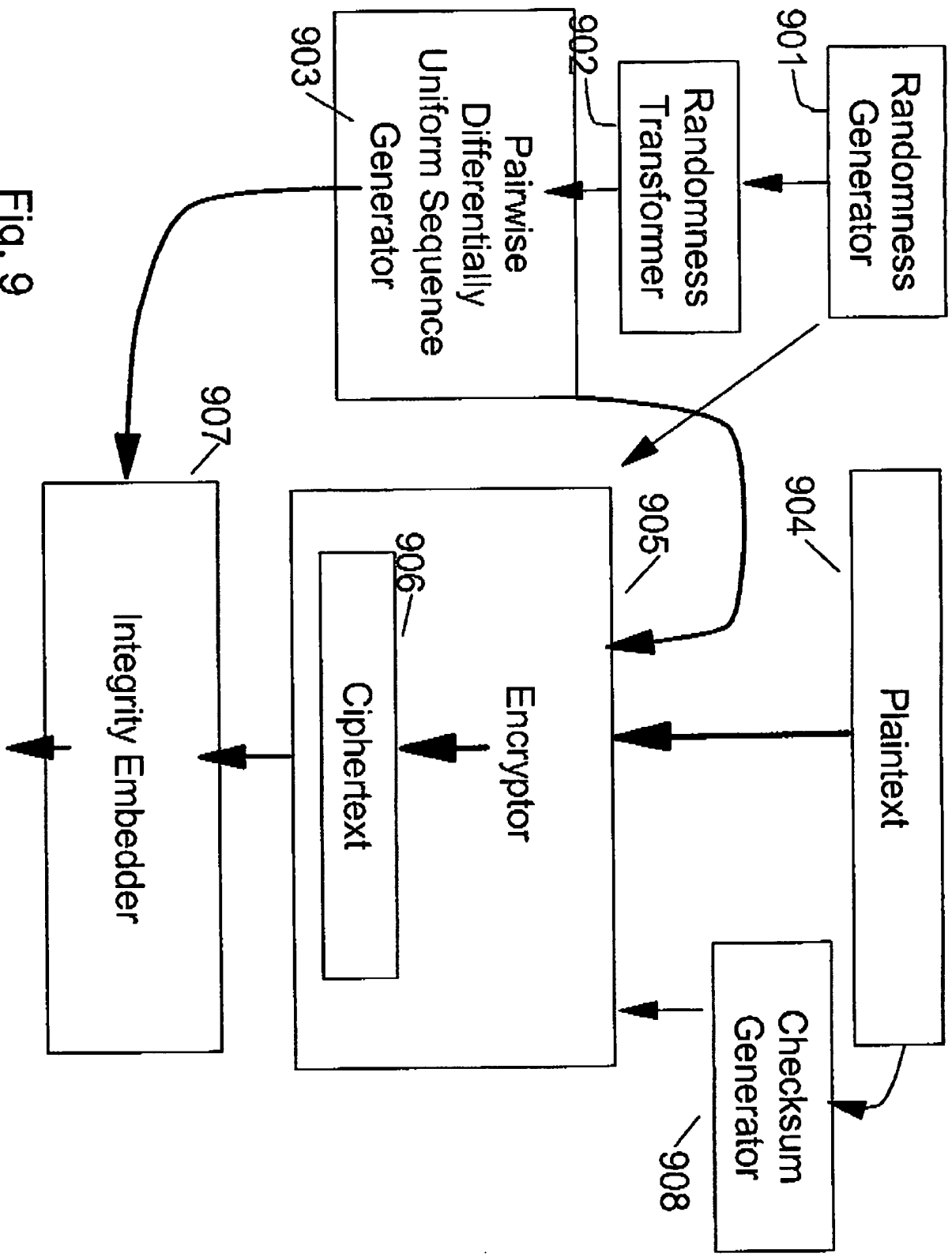
900
Randomness Generator
901
Randomness Transformer
902
Pairwise Differentially Uniform Sequence Generator
903
Plaintext
904
Encryptor
905
Ciphertext
906
Integrity Embedder
907
Checksum Generator
908

Fig. 9

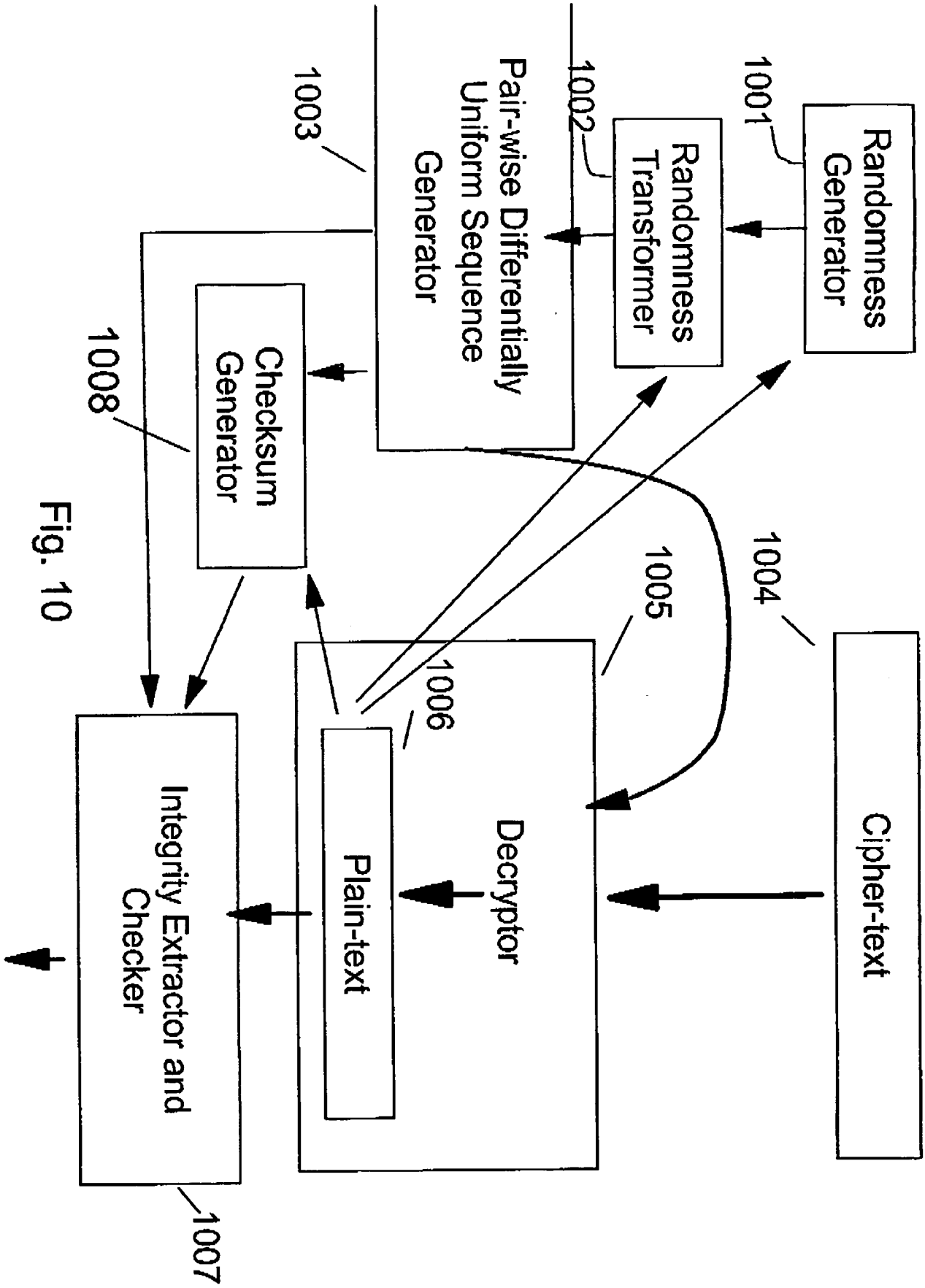
1000
Randomness Generator
1001
Randomness Transformer
1002
Pair-wise Differentially Uniform Sequence Generator
1003
Cipher-text
1004
Decryptor
1005
Plain-text
1006
Integrity Extractor and Checker
1007
Checksum Generator
1008

Fig. 10

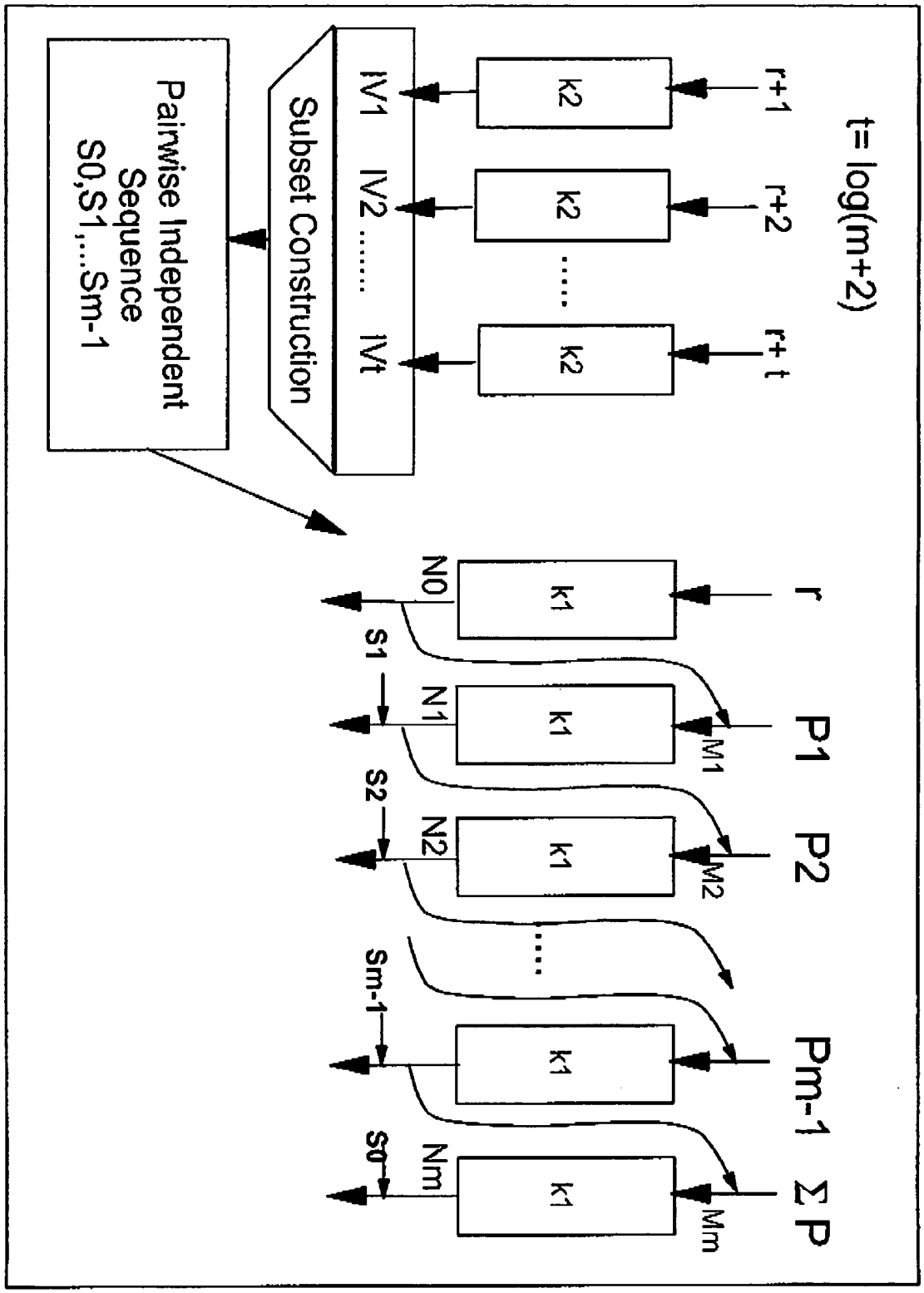
t= log(m+2)
r+1
r+2
r+ t
k2
k2
k2
IV1 IV2 ..... IVt
Subset Construction
Pairwise Independent Sequence
S0,S1,...Sm-1
r
P1
P2
Pm-1 ΣP
k1
N0
S1
N1
M1
S2
N2
M2
Sm-1
Nm
S0
Mm

Fig. 11

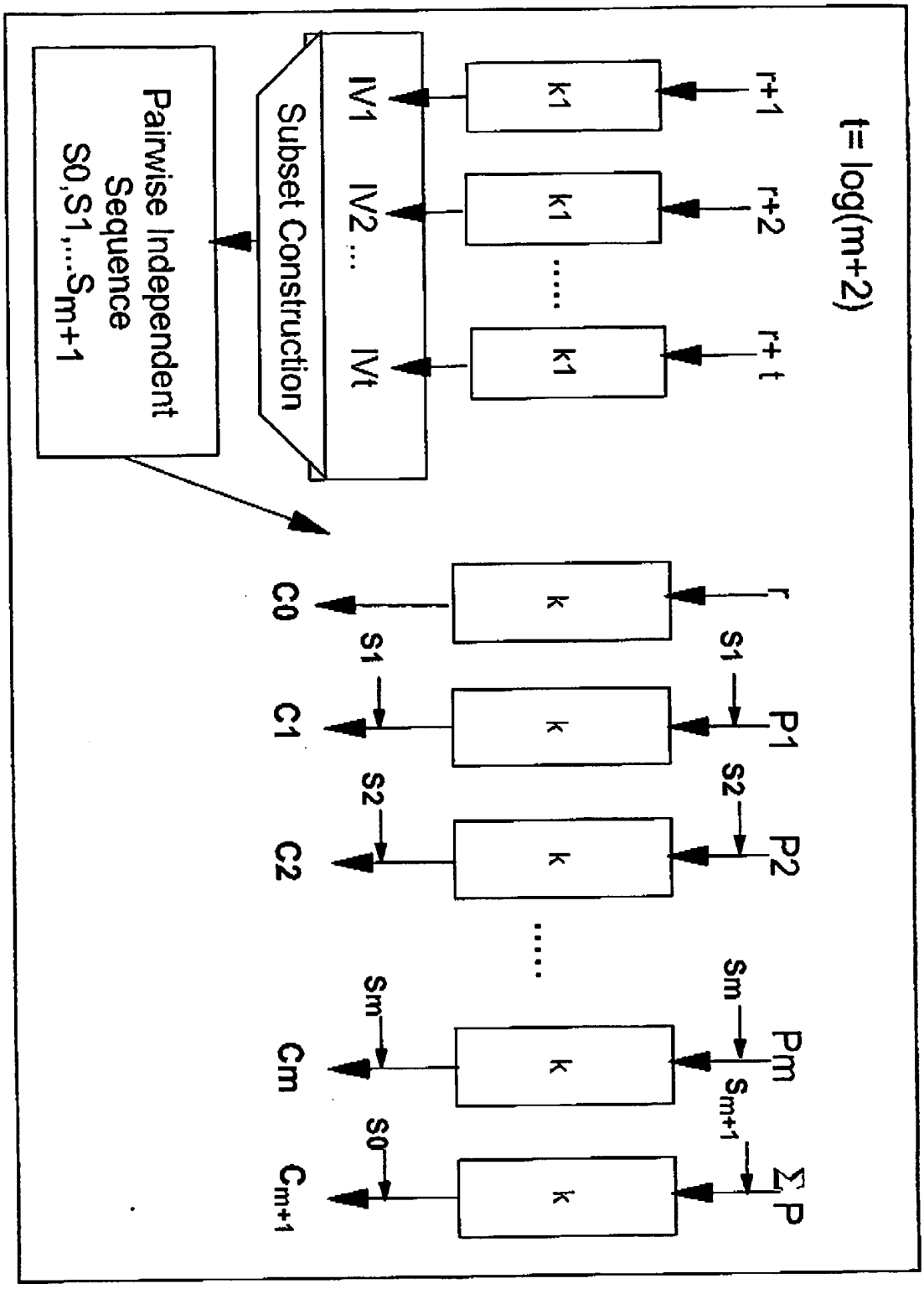
t= log(m+2)
r+1
r+2
r+ t
k1
k1
k1
IV1
IV2 ...
IVt
Subset Construction
Pairwise Independent Sequence
S0,S1,...Sm+1
r
S1
S2
Sm
S0
k
k
k
k
k
C0
C1
C2
Cm
Cm+1
S1
S2
Sm
Sm+1
P1
P2
Pm
ΣP

Fig. 12